



CVE-2016-0721

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2016-0721 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2017-04-21 15:59:00 UTC |
| Updated | 2023-02-12 23:15:00 UTC |
| Description | Session fixation vulnerability in pcsd in pcs before 0.9.157. |

Risk And Classification

Problem Types: CWE-384

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|----------------------------------|---------|--------|---------|----------|
| Application | Clusterlabs | Pcs | All | All | All | All |
| Operating System | Fedoraproject | Fedora | 22 | All | All | All |
| Operating System | Fedoraproject | Fedora | 23 | All | All | All |
| Operating System | Fedoraproject | Fedora | 22 | All | All | All |
| Operating System | Fedoraproject | Fedora | 23 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|---|----------------|
| CVE-2016-0721 - Red Hat Customer Portal | MISC | access.redhat.com | |
| [SECURITY] Fedora 22 Update: pcs-0.9.149-2.fc22 | FEDORA | lists.fedoraproject.org | Third Party Ad |
| pcs daemon CVE-2016-0721 Session Fixation Vulnerability | BID | www.securityfocus.com | Third Party Ad |
| Red Hat Customer Portal | MISC | access.redhat.com | |
| Red Hat Customer Portal | REDHAT | rhn.redhat.com | Third Party Ad |
| Bug 1299615 – CVE-2016-0721 pcs: cookies are not invalidated upon logout | CONFIRM | bugzilla.redhat.com | Issue Tracking |
| web UI auth: add js/ajax login dialog · ClusterLabs/pcs@acdbbe8 · GitHub | CONFIRM | github.com | Patch |
| web UI auth: decouple auth user from session · ClusterLabs/pcs@ba6ad90 · GitHub | CONFIRM | github.com | Patch |

| | | | |
|---|---------|---|----------------|
| web UI auth: decouple auth_user from session · ClusterLabs/pcs@b00a090 · GitHub | CONFIRM | github.com | Patch |
| [SECURITY] Fedora 23 Update: pcs-0.9.149-2.fc23 | FEDORA | lists.fedoraproject.org | Third Party Ad |
| web UI auth: store session data on server side · ClusterLabs/pcs@e9b2883 · GitHub | CONFIRM | github.com | Patch |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, ana |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report